AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An architecture for confirming the identity of a message sender on a remote services system, comprising:

a communications module operable to transmit a message;

a cryptographic module in said communication module for providing encryption of a data stream in said message;

a mid-level manager operating in conjunction with said communications module for controlling the flow of messages in said remote services system and for verifying the identity of a sender by comparing first and second data identities in said data stream, wherein said first data identity comprises data in a network software layer, said second data identity comprises data in an application software layer.

2. (canceled)

3. (Original) The architecture according to claim 2, said cryptographic module employing secure socket layer encryption.

4. (Original) The architecture according to claim 2, said mid-level manager controlling data flow between a customer proxy and an applications server.

5. (Original) The architecture according to claim 4, wherein said mid-level manager is a customer mid-level manager.

6. (Original) The architecture according to claim 4, wherein said mid-level manager is an aggregation mid-level manager.

7. (Original) The architecture according to claim 2, wherein transmission of said message is conditioned on HTTP.

8. (Original) The architecture according to claim 2, wherein transmission of said message is conditioned on email protocol.

9. (Currently Amended) A method of confirming the identity of a message sender on a remote services system, comprising:

obtaining a first identity related to a message, said first identity being obtained from a ~~first~~ network software layer in said remote services system;

obtaining a second identity related to the sender of a messages, said second identity being obtained from ~~a second~~ an application software layer in said remote services system; and

comparing said first identity with said second identity to verify the identity of the sender of said message.

10. (Canceled)

11. (Original) The method according to claim 10, further comprising encrypting said message and said identities in an encryption module in said remote services system.

12. (Original) The method according to claim 11, said encryption of said data and said identities being performed in accordance with secure socket layer protocol.

13. (Original) The method according to claim 12, said message being transmitted in said system using HTTP protocol.

14. (Original) The method according to claim 12, said message being transmitted in said system using email protocol.

15. (Currently Amended) A method of confirming the identity of a message sender on a remote services system, comprising:

transmitting a message using a communications module of said remote services system;

encrypting a data stream in said message using an encryption module in said communications module; and

controlling the flow of said message in said remote services system using a mid-level manager, said mid-level manager verifying the identity of a sender

by comparing first and second data identities in said data stream, wherein said first identity comprises encrypted data in a network software layer of said remote services system, said second identity comprises encrypted data in an application software layer of said remote services system.

16. (Canceled) The method according to claim 15,.

17. (Original) The method according to claim 15, said encryption module using secure socket layer protocol to encrypt said data stream.

18. (Original) The method according to claim 17, said mid-level manager controlling data flow between a customer proxy and an applications server.

19. (Original) The method according to claim 15, wherein said mid-level manager is a customer mid-level manager.

20. (Original) The method according to claim 15, wherein said mid-level manager is an aggregation mid-level manager.